REMARKS

In response to the Final Office Action dated 3-4-2010, the application has been amended within the advisory period to place the claims in condition for allowance or appeal. Review and reconsideration are requested in view of the above amendments and following remarks.

The examiner rejected claims 1, 2, 9, 11, 12, 19, 24-26 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is stated:

Regarding claims 1, 11, and 24, the examiner notes that the amended recitations of "operably residing therewith" and "operably residing with" lack antecedent basis within the applicant's disclosure. The examiner respectfully reminds the applicant that claims must conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description (see 37 CFR § 1.75). In the instant case, the examiner points out that the recitations in question render the claims ambiguous and the applicant's specification fails to provide clear direction as to their interpretation.

For example, the examiner points out that it is unclear whether the applicant's use of "operably residing" with/therewith is an attempt to reference a physical location of software or a reference to the software's state of cooperation or dwelling in league with the computer. The examiner further points out that applicant's remarks fail to address these amended recitations. The examiner notes that the applicant's original disclosure states that each of the various software modules or components (e.g. SSLAC, SSLAS) may be physically located or off-loaded onto one or more intermediary devices within the system (i.e. the SSLAC and SSLAS are located on an intermediary computer within the system - Specification, pg. 8). Thus, the examiner notes that the recitations "operably residing" with/therewith would appear to properly be interpreted as a reference to the software components' or modules' state of cooperation with the rest of the system components as opposed to a reference of a particular physical location of the components.

Regarding claims 1 and 11, the examiner notes that the recitation "the SSL acceleration client software on said client computer" (claim 1, line 19; claim 11, line19,20) lacks antecedent basis within the claim terminology. For the purpose of examination, the examiner presumes the applicant to recite `The SSL acceleration client software operably residing with said client computer". All depending claims are rejected by virtue of dependency.

Applicants have amended the application to state "disposed thereon" as opposed to "residing therewith" and this language is clearly in the specification, page 5, lines 10 and11 and in the drawings see FIG. 2A, for example. This is believed to overcome the 112 rejection and withdrawal of the rejection is requested.

Turning now to the substantive rejection wherein the examiner state Claims 1, 2, 11, 12, 24, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al. (Aziz), "Method and Apparatus for Providing Secure Communication with a Relay in a Network", U.S. Patent 6,643,701 in view of Gast, "System and Method for Accelerating Cryptographically Secured Transactions", U.S. Patent Publication 2003/0046532.

The examiner states:

Regarding claim 24, the examiner notes that Aziz discloses a system, comprising a client, server, and intermediary devices for establishing first (fig. 4:410) and second (fig. 4:460) SSL connections between a client and a server. The system comprises software components of SSL protocol server software" (Aziz, 6:21-24) and SSL protocol client software" (Aziz, 6:18-21) . However, Aziz does not appear to discuss the notion of SSL acceleration. Therefore, Aziz does not appear to disclose the recited software components of SSL acceleration server software and SSL acceleration client software.

Gast discloses the advantage of employing software components for SSL acceleration upon an intermediary device within a system for enabling SSL connections between a client and server. It would have been obvious to one of ordinary skill in the art to recognize the benefits of acceleration as disclosed by Gast within the system of Aziz. This would have been obvious because one of ordinary skill in the art would have been motivated by the advantages of speed and efficiency" The combination of Aziz and Gast enable [the claimed invention].

Applicants respectfully traverse. The object of both Aziz and Gast inventions is to provide a system wherein acceleration is an encryption offload service. That is, there is a front-end server which introduces an efficiency by performing encryption in hardware and offloading the content server. This has absolutely nothing to do with the efficiency taught by the instant invention, in which the SSL connection is terminated at the client computer by the SSL

acceleration client software (SSLAC) using the credentials of the content server's certificate for the purpose of putting the SSL transactions in the clear so that advanced data compression and elimination of application level handshakes can be performed over a second SSL communication link (or tunnel) between the SSLAC and the SSL acceleration server software (SSLAS). In the instant invention, the SSL acceleration client software communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software through SSL acceleration server software for validation thereof (thus putting communications in the clear) for enabling a second SSL connection with the first SSL connection between the client computer and the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer and which permits optimization techniques to be applied on data transmitted through the second SSL connection. In the Aziz/Gast cases, the acceleration is merely taught to be an encryption offload service. In the instant invention the actual data communications between the client and the data center is optimized. So this is a fundamental difference which is not taught by either Aziz or Gast.

The examiner goes on to state:

The combination of Aziz and Gast enable a web server having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key (fig 3:340, 4:470; 6:21-25; 5:6-13) , SSL acceleration software operably associated with said web server computer (Gast, fig 2:214; par. 34; Aziz, fig. 4:440; 5:6-13) which includes a pseudo CA certificate and access to said private key and a public key. Herein, the combination enables an intermediary comprising server acceleration software with access to the server's private key, certificate and a public key for the purpose of functional acceleration within SSL.

and a second computer communicatively linked to said web server computer (Aziz, fig. 4:420) operably associated with web browser software having SSL protocol client software

operably residing (Aziz, 6:18-21 herein Aziz discloses a client comprising software for enabling an SSL connection) therewith for enabling said first SSL connection between a client computer and said web server computer, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably residing with said client computer (Aziz, fig 4:420) wherein said SSL acceleration software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof (Aziz, 5:6-13, 41-65) for enabling a second connection (Aziz, fig. 4:460) with said first SSL connection (Aziz, fig. 4:410) between said client computer and said web server computer, wherein said second SSL connection is established between SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer (Aziz, 5:4-7 - herein, Aziz discloses that the server shares its private key with the "SSL acceleration server software" (e.g. relay) but not the "SSL acceleration client software" (E.g. proxy), and which permits optimization techniques to be applied on data transmitted through said SSL connection (Gast, fig 2:202, 214, 206, 212).

Again, the Gast figure cited teaches a cryptographic acceleration method. Aziz is teaching the same. Neither is teaching what is taught by the instant invention, in which the SSL connection is terminated at the client computer by the SSLAC using the credentials of the content server's certificate for the purpose of putting the SSL transactions in the clear so that advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SSLAC and the SSLAS. This is simply not taught at all by either Gast or Aziz.

The Examiner states:

Regarding claim 25, the combination enables: wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection (Aziz, 5:49-56; 8:66-9:13).

Aziz 5:49-56; 8:66-9:13 does not teach putting the traffic between the client computer and the proxy in the clear. It does teach putting the traffic between the relay and the web server

in the clear, which is the point of the cryptographic offload. In contrast, the applicant's instant invention does put the SSL traffic in the clear for the purposes of injecting advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SLAC and the SLAS. This is not taught, suggested or disclosed by the art in any way.

The examiner states:

"Regarding claims 9, 19 and 26, the combination recites software for transforming SSL data transmissions, but does not appear to explicitly recite compression."

Applicants' response to this: Of course it doesn't recite compression because the purpose of the cited inventions is to inject an encryption offload service in order to reduce the load on the web content server, whereas the purpose of the instant invention, which unlike the inventions cited, puts the SSL traffic in the clear for the purposes of injecting advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SLAC and the SLAS. Nowhere in the cited invention is that sort of "transformation" taught.

The examiner states:

"Freed, however teaches that SSL data transmissions are transformed by compression (Freed, par 10,52).

Here, the examiner is latching on to Freed's writings that a "compression method" is one of the negotiated aspects when setting up an SSL connection. The applicant is aware that a compression method is part of the SSL negotiations. However, one skilled in the art would

realize that there is much more to advanced data communications optimization than negotiating a compression method. Since a compression method has always been a basic part of SSL handshaking negotiations, the instant invention would be completely unnecessary if this compression method provided all the benefits of the instant invention. The reality is that there is a need for more sophisticated compression than that which is inherent in SSL and in fact the built-in compression methods which can be negotiated in an SSL handshake are rarely used. The instant invention provides more sophisticated compression methods which include not only reduction of data transfer but also elimination of application level hand-shakes. The fact that Freed cites a well-known facet of SSL communications is irrelevant since SSL is a fundamental part of the operating environment of the instant invention. Freed (like Aziz and Gast) does not teach putting the SSL traffic in the clear for the purposes of injecting advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SLAC and the SLAS. Notably, there is no teaching wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software and which permits optimization techniques to be applied on data transmitted through the second SSL connection.

The examiner states:

"It would have been obvious to one of ordinary skill in the art to employ compression within the SSL data transmission of the combination of Aziz and Gast. This would have been obvious because one of ordinary skill in the art would have been motivated by the teachings of the prior art regarding the nature of SSL transmissions.

This might be if the cited inventions can simply negotiate the data compression features of SSL, which simply compresses the payload as part of the encryption process. However, advanced data compression techniques require putting the data in the clear at the client. Unlike the prior art which completely lacks such teaching, the instant invention provides advanced data compression techniques which include functions like cache differencing and elimination of application level handshakes. None of the invention cited teach putting the SSL traffic in the clear by means of providing:

> "A system for increasing data access in a secure socket layer network environment, which includes:
>
> a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key; and
>
> a client computer communicatively linked to the web server computer having web browser software having SSL protocol client software operably disposed thereon for enabling the first SSL connection between the client computer and the web server, wherein the first SSL connection is established between the web browser software and SSL acceleration client software operably disposed thereon the client computer, wherein the SSL acceleration client software communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection with the first SSL connection between the client computer and

the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer and which permits optimization techniques to be applied on data transmitted through the second SSL connection"

for the purposes of injecting advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SSLAC and the SSLAS.

The examiner argues as follows:

The applicant essentially argues or asserts that: The prior art only suggests forming multiple SSL connections wherein the CA certificate including all components access to the private key and a public key exist in each instance of forming such connections which however in so doing would violate the SSL paradigm in the case of performing data optimization operations between a server and client. In contrast, the instant invention does not transmit the private key to preserve the SSL paradigm and yet enables optimization techniques to be performed through the second SSL connection between client and server.

As to the Examiner's remarks, the above statement by the examiner is not an accurate assessment of what was argued in the Applicant and Examiner's prior interview which took place in December 2009. At the interview it was stated that the private key is never transmitted from the SLAS to the SLAC. The teachings of the instant invention make it abundantly clear the private key is made accessible to the SLAS, otherwise the instant invention would be implausible.

The examiner states:

The examiner respectfully notes that the applicant's new and amended claims appear to recite a system comprising a client, server, and one or more intermediary devices for enabling the recited "first SSL connection" and "second SSL connection" The applicant asserts that "the instant invention does not transmit the private key", however the examiner respectfully points

disagrees. It is noted that the instant invention does in fact transmit or share the private key of the server with the intermediary SSLAS. Thus, the applicant's invention does not appear to distinguish over the prior art's disclosure of sharing the private key with the SSLAS (i.e "relay) (Aziz, 5-17).

To this, Applicants responds as follows. The teachings of the instant invention make it very clear that the private key is shared between the SSLAS and the content server. However what distinguishes the instant invention between the prior art cited and all other known prior art, is that the instant invention is able to terminate the SSL connection at the client using the credentials of the web server but without transferring the private key over to the client. This key distinguishing function is implemented without violating the SSL paradigm because all of the underlying communications which make this feat possible are done through the second SSL connection , i.e., the second SSL connection has been further characterized to be formed in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer. This is not taught anywhere but in the instant invention.

The references were discussed as lacking the now claimed structure. Namely, there is no disclosure, suggestion or teaching in the art, alone or in combination, of the system or method now recited.

The claimed invention is not shown, taught or suggested in the prior art. The prior art only suggests forming multiple SSL connections wherein the CA certificate including all components access to the private key and a public key exist in each instance of forming such connections which however in so doing would violate the SSL paradigm in the case of performing data optimization operations between a server and client.

In contrast, the instant invention does not transmit the private key to preserve the SSL paradigm and yet enables optimization techniques to be performed through the second SSL

connection between the client and server by virtue of terminating the SSL connection at the client using the credentials of the web server but without transferring the private key over to the client.

The amendment is not believed to raise any new issue which requires further search or consideration but only a change to comport with examiner's request to comply with antecedent basis issues and are submitted for purposes of simplifying the issues for review in order to gain allowance or place the claims in condition for appeal. Allowance of the claims is kindly requested at as early a date as possible. This is intended to be complete response to the Official Action dated 3/4/2010.

Respectfully submitted,

/R. William Graham/

R. William Graham, 33,891

Certificate of Transmission

I hereby certify that this correspondence is being electronically filed with the PTO for group 2437 on the date shown below.

/R. William Graham/

Date- Friday, April 16, 2010

R. William Graham, 33,891